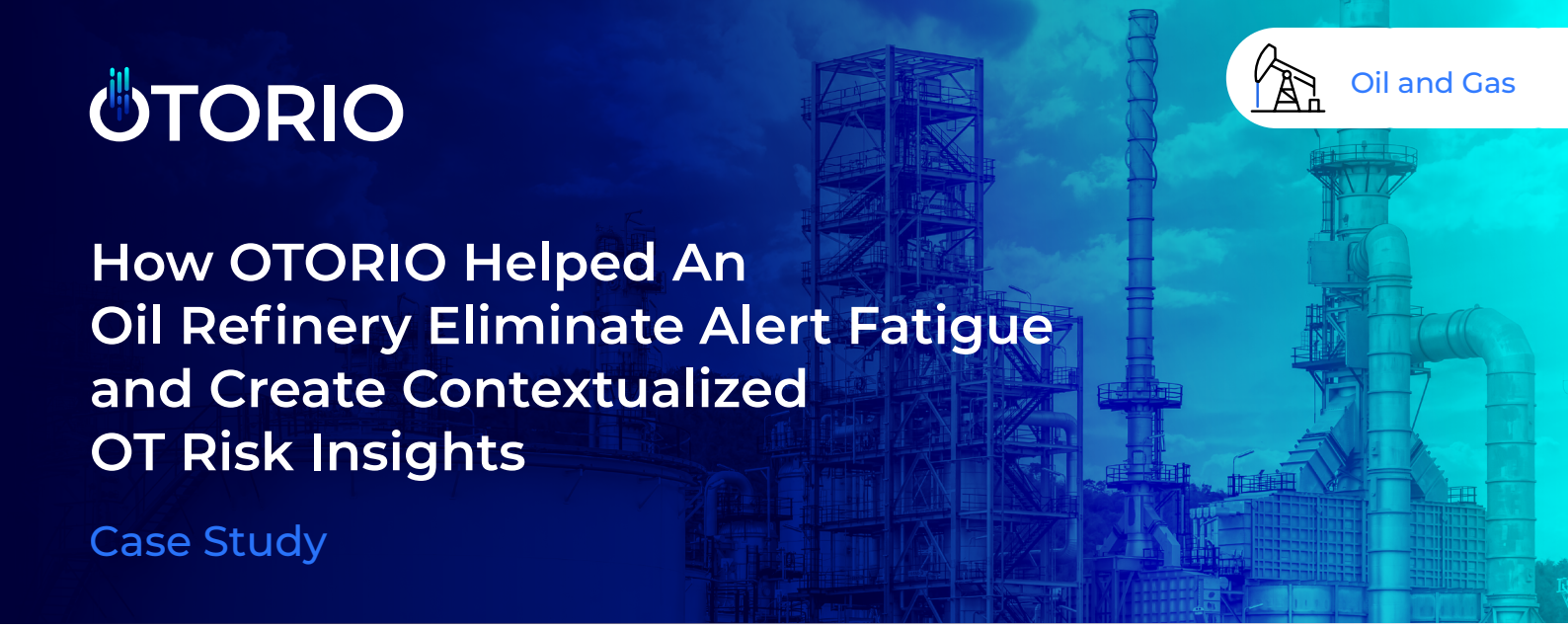
OTORIO

Oil and Gas

How OTORIO Helped An Oil Refinery Eliminate Alert Fatigue and Create Contextualized OT Risk Insights

Case Study



Reduced Noise from existing IDS

The company is an energy petrochemical refinery with geographically dispersed assets for petroleum refining, logistics, asphalt, renewable fuels, and retail convenience stores. Although it invested in OT cyber security solutions, the company's security team experienced alert fatigue due to the high volume of false-positive security notifications from its existing Intrusion Detection System (IDS). It also had challenges with its OT cyber security posture because it lacked asset visibility over all of the company's geographically scattered and unmanned environments. The sheer volume of alerts, combined with an inability to recognize real high-priority security threats with its existing resources, was a major challenge that the team needed to solve.

The company contacted OTORIO for an efficient and effective solution to:

- Reduce security-notification volume
- Support its security team with a 360° risk management view
- View the OT environment
- Simplify its OT cyber security management
- Discover and inventory all of its OT assets
- Identify risks and vulnerabilities

Customer Challenges

- An existing IDS created a high volume of ghost assets and false-positive alerts. These alerts made it much harder to detect and proactively respond to actual threats, causing alert fatigue for the refinery's cyber security team.
- An inability to prioritize risk effectively and efficiently, including discerning which alerts required immediate attention so that it could accurately detect and proactively respond to actual OT security risks.
- An inability to connect and leverage data sources and existing technologies to properly understand and secure its operational environment.

Advantages

As a holistic and agile solution, OTORIO's RAM² platform simplified the Energy company's OT cyber security management. It enabled security teams to:

- Discover all OT assets
- Identify risks
- Improve ROI on existing security controls
- Reduce the volume of security notifications
- Eliminate False-Positive security notifications
- Provide management overview of the OT environment

OTORIO's Solution

OTORIO's RAM² (Risk Assessment, Monitoring, and Management) solution helped the energy company automate and correlate events for fast and easy operational risk identification and noise suppression. RAM² was able to **enrich OT asset inventory and overview** by integrating with the company's:

- Existing firewall
- Passive monitoring, and re-using existing SPAN ports
- OT IDS
- Large automation vendor DCS
- EDRs
- Deploying Safe Active Query

Connecting to different data sources provided valuable, in-depth information about the refinery's OT environment:

- RAM² identified over 12,000 alerts as ghost assets, external (cloud) assets, and "out-of-working hours" alerts, even though the refinery operates 24/7 with U.S. and international security teams operating in different time zones, all alerts were created by the company's existing IDS solution.
- RAM² managed to transform how data sources were presented to **show only legitimate, relevant alerts of highly impactful assets** in addition to repetitive and abnormal behavior alerts that needed to be addressed.
- **RAM² enriched asset attribution with operational context**, known vulnerabilities, and a comprehensive assessment of security posture controls and compliance.
- RAM² proactively **identified exposures** by analyzing the correlation between security posture and asset inventory. The correlation of various events based on OT assets delivered RAM² insights that enabled the company to **prioritize risks, corresponding mitigation steps**, and required resources. This significantly reduced the amount of noise generated by the client's existing IDS solution.

What is OT Security Context?

To provide risk-based OT security situational awareness, Operational Technology (OT) Security Context analyze together a rich set of security and industrial data sources and takes into consideration:

- Asset or a group of assets impact (e.g., vulnerabilities, communication paths, asset relationships, exposure, and discovery).
- Potential business and operational impact on processes (i.e., production, safety, financial, environmental, and regulatory matters).

Less noise. More context

Raw asset information
PLCs, RTUs, Sensors

Security systems
EDR, Firewall, NAC, AD, SRA

Industrial solutions
OPC, DCS, Historian

Logs
Windows event logs, Servers, HMI

Network monitoring
IDS, Traffic, Netflow

27,000+ Events
Excluding: Ghost | External | Multicast | Broadcast assets

2,441 Indicators
Turn data source legitimate alerts into indicators (non-working hours, legitimate tasks got verified, etc.)

76 Alerts
Represent alerts that should be addressed or checked (repetitive, high impactful assets, abnormal behavior)

29 Insights
Correlate insights based on indicators and alerts (pattern based analysis, defined insights, etc.)

- **Improved MTTD** (Mean Time To Detect)
- **Improved MTTR** (Mean Time To Response) with automated mitigation steps
- **OT** context-based **prioritization**

OTORIO

Oil and Gas

Benefits for the Oil Refinery

- It now has a **unified risk view of converged OT-IT-IIoT network** security systems within its OT environment.
- It **improved its ROI for pre-existing security controls** and solutions by integrating them with OTORIO's RAM² platform to leverage the refinery's technology investments.
- The refinery's security teams have **OT operational context and impact analysis** of an asset or process-level for OT risk-based management.
- OTORIO's RAM² provides them with insights that **improved the company's Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR),** while reducing noise and highlighting what risks and vulnerabilities should be prioritized.
- The OT security platform enabled the energy company to conduct **safe operational security posture assessments** without disturbing ongoing operations.
- The oil refinery obtained a comprehensive security assessment report, providing senior management with a **full picture of the company's OT cyber security posture.**
- Teams now have quick **risk mitigation playbooks with clear instructions**, and they hardened site-specific OT network risks and vulnerabilities.
- The energy company is proactively becoming **"ransomware ready"** by automating gaps and exposure analysis to reduce OT security risks.
- OT security compliance and auditing processes are now automated, enabling the company to know and understand its **OT compliance with industry and market standards.**

About OTORIO

OTORIO has pioneered an industrial-native OT security platform that enables its customers to achieve an integrated, holistic security strategy for industrial control systems (ICS) and cyber-physical systems (CPS).

Together with its partners, OTORIO empowers operational security practitioners to proactively manage cyber risks and ensure resilient operations. The company's platform provides automated and consolidated visibility of the entire operational network, enabling companies to take control of their security posture, eliminate critical risks, and deliver immediate business value across the organization.

OTORIO's global team combines the extensive mission-critical experience of top nation-state cyber security experts with deep operational and industrial domain expertise.

otorio.com

Catalog number: 220522